Does Information Security Exist?

Brad Weakly

State of Nebraska – Office of the CIO

brad.weakly@nebraska.gov

What is information Security?

- An all encompassing term that refers to the security of the information systems that are used and the data that is processed.
- Preservation of the confidentiality, integrity and availability of information.
- Situation in which information security risks are under control.
- The implementation of programs and practices that protect the integrity and safety of computer programs and information.

Risk and Preparedness

- Risk – The relative likelihood that a bad thing will happen
- Preparedness – The state of being prepared for specific or unpredictable events or situations
- Preparedness is never 100%
- Security is about preparing for events, reducing the risk and accepting residual risk

Risk and exposure

- Risk comes in many forms. Risk management is about accepting your level of risk across multiple areas.
- Have you identified each area of possible exposure? Have you considered your exposure to insider threat?
- Are you comfortable that your risk level is acceptable?

Security must be non-stop

- Cyber security is a 24x7x365 endeavor.
- We staff based on extended workday hours, typically with a reduced staff after hours and on weekends.
- World time doesn’t honor time zones; it doesn’t recognize weekends or holidays.
- Do traditional crimes occur more during the 8-5 work day or after hours?

Compromise

- How many of you have had a system that has been infected or compromised?
- How many of you know of someone personally who has been infected or compromised?
- How many of you know or have heard of someone who has been infected or compromised?

The human side

- Are you still feeling secure?
- Human nature is a wonderful awful thing!
- We have a tendency to disassociate ourselves from information and news that could point out or cause us harm.

Security coverage

- The difficulty in identifying and assessing the level of risk under changing conditions.
- The “Security Blanket” of the past leaves a few appendages exposed today – it will leave us half-naked tomorrow unless we adapt.

Security in the past

- Remember when:
  - A locked door was the equivalent of an open/closed sign.
  - When “bad guys” wore masks.
  - Potential loss was what someone could carry out with their hands.
  - Foreign incidents were things that happened somewhere else.

The world is very, very close

- The internet is no longer for the sole use of government, universities and research – it becomes commercial.
- Emergence of browsers and the world-wide-web.
- Email became a valuable and useful communications tool.
- Worms and viruses popped into existence, and we made up catchy names like SPAM to describe the not so tasty new side of email.

Security history

- What is the point of rehashing history?
- What is the point that needs to be made?
- What does this have to do with current security?

Present day security

- Congratulations! You have made it through to today and have survived years of a changing security landscape.

Security in-depth

- Perimeter Security
- Security in layers
- Intrusion protection and prevention
- Event consolidation and correlation
- Security awareness

System and application patching

- Microsoft Patch Tuesday
  - Exploit Wednesday
  - General Operating System patching
  - Application patching
  - Lag between discovery, vendor fix and patching. Zero-day vulnerabilities are still an issue.

Zero day vulnerabilities and exploits

- No direct defense
- Are there limits on systems that access financial data or approve payments?
- Are critical systems isolated from users?
- Follow-up after detection of infected systems is crucial

Insider Threat

- Insider threat is one of the highest risk threats. A threat that also has a high likelihood of occurring!
- Background checks for employees based on the information they handle or have access to.

Advanced Persistent Threats (APT)

- Advanced Persistent Threats (APTs) are a cybercrime category directed at business and political targets. APTs require a high degree of stealthiness over a prolonged duration of operation in order to be successful. The attack objectives therefore typically extend beyond immediate financial gain, and compromised systems continue to be of service even after key systems have been breached and initial goals reached.

Advanced Persistent Threats (APT)

- **Advanced** – Criminal operators behind the threat utilize the full spectrum of computer intrusion technologies and techniques. While individual components of the attack may not be classed as particularly “advanced” (e.g. malware components generated from commonly available DIY construction kits, or the use of easily procured exploit materials), their operators can typically access and develop more advanced tools as required. They combine multiple attack methodologies and tools in order to reach and compromise their target.

Advanced Persistent Threats (APT)

- **Persistent** – Criminal operators give priority to a specific task, rather than opportunistically seeking immediate financial gain. This distinction implies that the attackers are guided by external entities. The attack is conducted through continuous monitoring and interaction in order to achieve the defined objectives. It does not mean a barrage of constant attacks and malware updates. In fact, a “low-and-slow” approach is usually more successful.

Advanced Persistent Threats (APT)

- **Threat** – means that there is a level of coordinated human involvement in the attack, rather than a mindless and automated piece of code. The criminal operators have a specific objective and are skilled, motivated, organized and well funded.

Denial of Service (DOS)

- DDOS – Distributed (popular) variant
- Financial and Reputation impact
- Cover for more covert activities
- Slowloris – Apache HTTP (web) Dos attack
  - More generic finite resource service attacks.

Future Risk

- Fast flux botnets
  - Fast flux is a technique used by some botnets, such as the Storm botnet, to hide phishing and malicious Web sites behind an ever-changing network of compromised hosts acting as proxies. Using a combination of peer-to-peer networking, distributed command-and-control, Web-based load balancing and proxy redirection, it makes it difficult to trace the botnet's original geo-location.

IPv6 Deployments

- Ethernet card vendor guess
- New attack vectors – All node/router addresses
- New multicast Addresses
- All nodes (FF02::1), all routers (FF05::2) and all DHCP servers (FF05::5)
- New application and OS vulnerabilities
- Mobile IP – MIPv6

Mobility

- Growing number of mobile users and devices
- Physical risk – theft or loss
- Operating system and Application risk
- Network/bluetooth connectivity risk
- Mobile data storage device risk
  - Massive storage capability enhances risk
  - Key vector for potential loss of confidential data

Socialization of IT

- Use of consumer services for business
- Use of Facebook, MySpace and Twitter
- Skype use blurs traffic analysis at the perimeter. Its encrypted traffic is generally incompatible with firewalls and traffic sensors.
- New avenues of employee and business exploitation

Our models are working right?

- Past performance is no guarantee of future success.
- Application vulnerabilities bypass the perimeter and make it directly to the desktop.
- Botnet hosts are low-key and very difficult to detect until mobilized – then it’s too late.
- Insider threat is real, take precautions.
- Mobile device use is accelerating.

Your users are your strength and your weakness

- Users need to be an integral part of security.
- Your cyber security profile is heavily dependent on what your users do.
- Anomalies need to be reported.
- Background checks need to be performed on personnel with access to sensitive systems and data.
- Treat your laptops like cash; treat your data the same way!

Change

- Cyber criminals are changing their tactics.
  - Exploiting lower risk vulnerabilities that are not patched as quickly as high risk vulnerabilities
  - Embracing social engineering methods
  - Starting to do their research
  - Targeting attacks based on publicly available information
  - Data mining for relevant information
  - They are sharing information!

Why current models will not carry us forward

- Cyber criminals are grouping together to share expertise and resources and to collaborate.
- Network enabled embedded devices are becoming commonplace – they are susceptible.
- The reason behind compromise has changed, now it’s all about the money.
- New modes of attack like firmware hacking are outside our current capability of detection.

What is different about protecting Critical Infrastructure and Key Resources ?

- The general idea is that key resources have a high likelihood of not being available during a major event or crisis.
- What you are doing for security and containment now is a very important indicator for how you can respond.
- Plan for those key resources to be unavailable and document your procedures for recovery.

There is strength in numbers

- It is a universal truth.
- Constrained budget – then reach out to others.
- Understaffed – then reach out to others.
- Missing some expertise – then reach out to others.
- Concerned that we need to do more – then reach out to others.

Is the threat increasing or decreasing?

- As the vectors increase and the expertise of the criminals increases, so does the threat.
- More devices are coming on-line, especially mobile devices.
- Increased use of IP enabled home devices such as media players and home theater.
- More users are using the Internet to access audio and video media.

Financial system compromise

- Compromise of electronic funds transfer process.
- Compromise of online-banking account information.

So what should we do?

- First we need to realize the threat is real and it exists right now. Without that realization there will be little action.
- We need to neutralize the fear of sharing cyber security related information.
- We need to enhance the coordination efforts between companies, cites, counties, the State and Federal government.
- We need to work more as a team.

Are you secure?

- What are you going to do to help address the increasing number and risk of security threats?
- Are you ready to participate? Are you willing to share information?
- Are you willing to change?

Does information security exist?

- Of course it does! Security isn't 100%, but we have a good track record and we are improving.
- We do need to realize this is not your problem, it is our problem.
- Minor security incidents might highlight the problem, but they also help us improve our methodology for the long-term win.

Resources

- SANS: www.sans.org
- Security Dark Reading: www.darkreading.com
- Packet Storm: www.packetstormsecurity.org
- Security Focus: www.securityfocus.com
- www.us-cert.gov
- www.cybercrime.gov

- 2010 Nebraska Cyber Security Conference:
  - http://its.ne.gov/cybersecurity/events

Thank you!

Brad Weakly
State of Nebraska – Office of the CIO

brad.weakly@nebraska.gov